

# National Cyber Alert System

[Archive](#)

## Cyber Security Bulletin SB10-011

### Vulnerability Summary for the Week of January 4, 2010

The US-CERT Cyber Security Bulletin provides a summary of new vulnerabilities that have been recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) in the past week. The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the [NVD](#), which contains historical vulnerability information.

The vulnerabilities are based on the [CVE](#) vulnerability naming standard and are organized according to severity, determined by the [Common Vulnerability Scoring System](#) (CVSS) standard. The division of high, medium, and low severities correspond to the following scores:

- **High** - Vulnerabilities will be labeled High severity if they have a CVSS base score of 7.0 - 10.0
- **Medium** - Vulnerabilities will be labeled Medium severity if they have a CVSS base score of 4.0 - 6.9
- **Low** - Vulnerabilities will be labeled Low severity if they have a CVSS base score of 0.0 - 3.9

Entries may include additional information provided by organizations and efforts sponsored by US-CERT. This information may include identifying information, values, definitions, and related links. Patch information is provided when available. Please note that some of the information in the bulletins is compiled from external, open source reports and is not a direct result of US-CERT analysis.

High Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
awingsoft -- awakening_winds3d_player awingsoft -- awakening_winds3d_viewer	Heap-based buffer overflow in the WindsPlayerIE.View.1 ActiveX control in WindsPly.ocx 3.5.0.0 Beta, 3.0.0.5, and earlier in AwingSoft Awakening Web3D Player and Winds3D Viewer allows remote attackers to cause a denial of service (application crash) or execute arbitrary code via a long SceneUrl property value, a different vulnerability than CVE-2009-2386. NOTE: some of these details are obtained from third party information.	2010-01-07	9.3	<a href="#">CVE-2009-4588</a> <a href="#">XF</a> <a href="#">MISC</a> <a href="#">MILWoRM</a> <a href="#">SECUNIA</a>
cdmi -- a2_media_player_pro	Stack-based buffer overflow in A2 Media Player Pro 2.51 allows remote attackers to execute arbitrary code via a long string in a (1) .m3u or (2) .m3l playlist file.	2010-01-04	9.3	<a href="#">CVE-2009-4549</a> <a href="#">MILWORM</a>
cmstactics -- com_beeheard	SQL injection vulnerability in the BeeHeard (com_beeheard) component 1.x for Joomla! allows remote attackers to execute arbitrary SQL commands via the category_id parameter in a suggestions action to index.php.	2010-01-06	7.5	<a href="#">CVE-2009-4576</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">OSVDB</a> <a href="#">MISC</a> <a href="#">SECUNIA</a> <a href="#">MISC</a>

dbmasters -- db_masters_multimedia_links_directory	admin.php in dB Masters Multimedia Links Directory 3.1.3 allows remote attackers to bypass authentication and gain administrative access via a certain value of the admin_log cookie.	2010-01-06	7.5	CVE-2009-4584 BID OSVDB SECUNIA MISC
elkagroup -- image_gallery	SQL injection vulnerability in elkagroup Image Gallery allows remote attackers to execute arbitrary SQL commands via the id parameter to the default URI under news/.	2010-01-05	7.5	CVE-2009-4569 XF BID MISC MISC
i-escorts -- i-escorts_directory_script	SQL injection vulnerability in country_escorts.php in I-Escorts Directory Script allows remote attackers to execute arbitrary SQL commands via the country_id parameter.	2010-01-06	7.5	CVE-2009-4574 XF OSVDB MISC SECUNIA MISC
intesync -- miniweb	SQL injection vulnerability in the Survey Pro module for Miniweb 2.0 allows remote attackers to execute arbitrary SQL commands via the campaign_id parameter in a results action to index.php.	2010-01-04	7.5	CVE-2009-4551 BID MILWoRM
joomla -- com_dhforum	SQL injection vulnerability in the DhForum (com_dhforum) component for Joomla! allows remote attackers to execute arbitrary SQL commands via the id parameter in a grouplist action to index.php.	2010-01-06	7.5	CVE-2009-4583 XF BID MISC MISC
joomlabamboo -- jb_simpla	SQL injection vulnerability in the JoomlaBamboo (JB) Simpla Admin template for Joomla! allows remote attackers to execute arbitrary SQL commands via the id parameter in an article action to the com_content component, reachable through index.php.	2010-01-06	7.5	CVE-2010-0158 VUPEN BID MISC MISC
joomlablestudy -- com_biblestudy	Directory traversal vulnerability in the Bible Study (com_biblestudy) component 6.1 for Joomla! allows remote attackers to include and execute arbitrary local files via a .. (dot dot) in the controller parameter in a studieslist action to index.php.	2010-01-06	7.5	CVE-2010-0157 BID SECUNIA MISC
maxdev -- mdforum	SQL injection vulnerability in the MDForum module 2.x through 2.07 for MAXdev MDPPro allows remote attackers to execute arbitrary SQL commands via the c parameter to index.php.	2010-01-06	7.5	CVE-2009-4577 XF BID OSVDB CONFIRM SECUNIA
	Multiple SQL injection vulnerabilities in index.php in PhpShop 0.8.1 allow remote attackers to execute arbitrary SQL commands via the (1) module_id parameter in an admin/function_list action, the (2) vendor_id parameter in a vendor/vendor_form action, the (3) module_id parameter in an admin/module_form action, the (4) user_id			CVE-2009-4571 VUL

phpshop -- phpshop	parameter in an admin/user_form action, the (5) vendor_category_id parameter in a vendor/vendor_category_form action, the (6) user_id parameter in a store/user_form action, the (7) payment_method_id parameter in a store/payment_method_form action, the (8) tax_rate_id parameter in a tax/tax_form action, or the (9) category parameter in a shop/browse action. NOTE: the product_id vector is already covered by CVE-2008-0681.	2010-01-05	7.5	<a href="#">XF</a> <a href="#">BID</a> <a href="#">BUGTRAQ</a> <a href="#">MISC</a> <a href="#">SECUNIA</a>
quickheal -- antivirus_plus_2009 quickheal -- total_security_2009	Quick Heal AntiVirus Plus 2009 10.00 SP1 and Quick Heal Total Security 2009 10.00 SP1 use weak permissions (Everyone: Full Control) for the product files, which allows local users to gain privileges by replacing executables with Trojan horse programs, as demonstrated by replacing quhlpvc.exe.	2010-01-04	7.2	<a href="#">CVE-2009-4556</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">BUGTRAQ</a> <a href="#">SECUNIA</a>
secureideas -- base	SQL injection vulnerability in Basic Analysis and Security Engine (BASE) before 1.4.4 allows remote attackers to execute arbitrary SQL commands via unspecified vectors.	2010-01-07	7.5	<a href="#">CVE-2009-4591</a> <a href="#">VUPEN</a> <a href="#">CONFIRM</a>
secureideas -- base	Unspecified vulnerability in base_local_rules.php in Basic Analysis and Security Engine (BASE) before 1.4.4 allows remote attackers to include arbitrary local files via unknown vectors.	2010-01-07	7.5	<a href="#">CVE-2009-4592</a> <a href="#">XF</a> <a href="#">VUPEN</a> <a href="#">CONFIRM</a> <a href="#">SECUNIA</a> <a href="#">CONFIRM</a>
sendmail -- sendmail	sendmail before 8.14.4 does not properly handle a '\o' character in a Common Name (CN) field of an X.509 certificate, which (1) allows man-in-the-middle attackers to spoof arbitrary SSL-based SMTP servers via a crafted server certificate issued by a legitimate Certification Authority, and (2) allows remote attackers to bypass intended access restrictions via a crafted client certificate issued by a legitimate Certification Authority, a related issue to CVE-2009-2408.	2010-01-04	7.5	<a href="#">CVE-2009-4565</a> <a href="#">VUPEN</a> <a href="#">CONFIRM</a>
worms-league -- webleague	SQL injection vulnerability in profile.php in WebLeague 2.2.0 allows remote attackers to execute arbitrary SQL commands via the name parameter.	2010-01-04	7.5	<a href="#">CVE-2009-4560</a> <a href="#">XF</a> <a href="#">MILWoRM</a>
xoops -- xoops_dictionary	SQL injection vulnerability in detail.php in the Dictionary module for XOOPS 2.0.18 allows remote attackers to execute arbitrary SQL commands via the id parameter.	2010-01-06	7.5	<a href="#">CVE-2009-4582</a> <a href="#">XF</a> <a href="#">BID</a> <a href="#">MISC</a>
zenphoto -- zenphoto	SQL injection vulnerability in index.php in Zenphoto 1.2.5 allows remote attackers to execute arbitrary SQL commands via the title parameter in a news action. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2010-01-04	7.5	<a href="#">CVE-2009-4566</a> <a href="#">XF</a> <a href="#">SECUNIA</a> <a href="#">OSVDB</a>

[Back to top](#)

Medium Vulnerabilities				
Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
aspindir -- uranyumsoft_listing_service	UranyumSoft Listing Service stores sensitive information under the web root with insufficient access control, which allows remote attackers to download a database via a direct request for database/db.mdb.	2010-01-06	5.0	CVE-2009-4585 XF OSVDB MISC SECUNIA MISC
cherokee -- cherokee	Cherokee Web Server 0.5.4 allows remote attackers to cause a denial of service (daemon crash) via an MS-DOS reserved word in a URI, as demonstrated by the AUX reserved word.	2010-01-07	5.0	CVE-2009-4587 XF MISC SECTRACK BID BUGTRAQ BUGTRAQ
facileforms -- facileforms	Cross-site scripting (XSS) vulnerability in the Facileforms (com_facileforms) component for Joomla! and Mambo allows remote attackers to inject arbitrary web script or HTML via the Itemid parameter to index.php.	2010-01-06	4.3	CVE-2009-4578 XF BID MISC MISC
forum.snitz -- snitz_forums_2000	Multiple cross-site scripting (XSS) vulnerabilities in Snitz Forums 2000 3.4.07 allow remote attackers to inject arbitrary web script or HTML via (1) the url parameter to pop_send_to_friend.asp, related to a crafted onload attribute of an IMG element; or (2) an onload attribute in a sound tag.	2010-01-04	4.3	CVE-2009-4554 XF XF VUPEN BID BUGTRAQ SECUNIA
hastablog -- hasta_blog	Multiple cross-site scripting (XSS) vulnerabilities in Hasta Blog 2.3 allow remote attackers to inject arbitrary web script or HTML via the id parameter to (1) yorumyaz.php and (2) blog.php.	2010-01-06	4.3	CVE-2009-4580 XF OSVDB MISC SECUNIA MISC
intesync -- miniweb	Cross-site scripting (XSS) vulnerability in the Survey Pro module for Miniweb 2.0 allows remote attackers to inject arbitrary web script or HTML via the PATH_INFO to index.php.	2010-01-04	4.3	CVE-2009-4552 BID MILWORM
jesse_smith -- bftpd	The bftpdutmp_log function in bftpdutmp.c in Bftpd before 2.4 does not place a '\0' character at the end of the string value of the ut.bu_host structure member, which might allow remote attackers to cause a denial of service (daemon crash) via unspecified vectors. NOTE: some of these details are obtained from third party information.	2010-01-07	5.0	CVE-2009-4593 VUPEN BID CONFIRM
joomla -- com_artistavenue	Cross-site scripting (XSS) vulnerability in the Artist avenue (com_artistavenue) component for Joomla! and Mambo allows remote attackers to inject arbitrary web script or HTML via the Itemid	2010-01-06	4.3	CVE-2009-4579 XF BID MISC

	parameter to index.php.		MISC MISC
joomlabear -- mod_joomulus	Multiple cross-site scripting (XSS) vulnerabilities in the Joomulus (mod_joomulus) module 2.0 for Joomla! allow remote attackers to inject arbitrary web script or HTML via the tagcloud parameter in a tags action to (1) tagcloud_ell.swf, (2) tagcloud_eng.swf, (3) tagcloud_por.swf, (4) tagcloud_rus.swf, and possibly (5) tagcloud_jpn.swf. NOTE: the provenance of this information is unknown; the details are obtained solely from third party information.	2010-01-06	4.3  CVE-2009-4573 XF OSVDB OSVDB OSVDB OSVDB SECUNIA
k-factor -- agoracart	Multiple cross-site request forgery (CSRF) vulnerabilities in AgoraCart 5.2.005 and 5.2.006 and AgoraCart GOLD 5.5.005 allow remote attackers to hijack the authentication of administrators for requests that (1) modify a .htaccess file via an unspecified request to protected/manager.cgi or (2) change the password of an administrative account.	2010-01-04	6.8  CVE-2009-4555 XF SECUNIA MISC
kingston -- datatraveler_blackbox kingston -- datatraveler_elite kingston -- datatraveler_secure	Kingston DataTraveler BlackBox (DTBB), DataTraveler Secure Privacy Edition (DTSP), and DataTraveler Elite Privacy Edition (DTEP) USB flash drives validate passwords with a program running on the host computer rather than the device hardware, which allows physically proximate attackers to access the cleartext drive contents via a modified program.	2010-01-07	4.6  CVE-2010-0221 MISC MISC MISC MISC MISC SECTRACK MISC MISC MISC
kingston -- datatraveler_blackbox kingston -- datatraveler_elite kingston -- datatraveler_secure	Kingston DataTraveler BlackBox (DTBB), DataTraveler Secure Privacy Edition (DTSP), and DataTraveler Elite Privacy Edition (DTEP) USB flash drives use a fixed 256-bit key for obtaining access to the cleartext drive contents, which makes it easier for physically proximate attackers to read or modify data by determining and providing this key.	2010-01-07	4.6  CVE-2010-0222 MISC MISC MISC MISC MISC MISC MISC MISC
kingston -- datatraveler_blackbox kingston -- datatraveler_elite kingston -- datatraveler_secure	Kingston DataTraveler BlackBox (DTBB), DataTraveler Secure Privacy Edition (DTSP), and DataTraveler Elite Privacy Edition (DTEP) USB flash drives do not prevent password replay attacks, which allows physically proximate attackers to access the cleartext drive contents by providing a key that was captured in a USB data stream at an earlier time.	2010-01-07	4.6  CVE-2010-0223 MISC MISC MISC MISC
liferay -- liferay_portal	Cross-site scripting (XSS) vulnerability in Liferay Portal before 5.3.0 allows remote attackers to inject arbitrary web script or HTML via the p_p_id parameter.	2010-01-07	4.3  CVE-2009-3742 CERT-VN CONFIRM
malcom_box -- lxr_cross_referencer	Cross-site scripting (XSS) vulnerability in LXR Cross Referencer 0.9.5 and 0.9.6 allows remote attackers to inject arbitrary web script or HTML via the i parameter to the ident program.	2010-01-07	4.3  CVE-2009-4497 MLIST SECUNIA
	Cross-site scripting (XSS) vulnerability in the		

mediawiki -- mediawik mediawiki -- mediawiki	Special:Block implementation in the getContribsLink function in SpecialBlockip.php in MediaWiki 1.14.0 and 1.15.0 allows remote attackers to inject arbitrary web script or HTML via the ip parameter.	2010-01-07	4.3	CVE-2009-4589 VUPEN BID
mozilla -- firefox	The nsObserverList::FillObserverArray function in xpcom/ds/nsObserverList.cpp in Mozilla Firefox before 3.5.7 allows remote attackers to cause a denial of service (application crash) via a crafted web site that triggers memory consumption and an accompanying Low Memory alert dialog, and also triggers attempted removal of an observer from an empty observers array.	2010-01-07	5.0	CVE-2010-0220 CONFIRM MISC
phpshop -- phpshop	Cross-site scripting (XSS) vulnerability in PhpShop 0.8.1 allows remote attackers to inject arbitrary web script or HTML via the order_id parameter in an order/order_print action to the default URI.	2010-01-05	4.3	CVE-2009-4570 XF BID BUGTRAQ MISC SECUNIA
phpshop -- phpshop	Cross-site request forgery (CSRF) vulnerability in PhpShop 0.8.1 allows remote attackers to hijack the authentication of arbitrary users for requests that invoke the cartAdd function in a shop/cart action to the default URI.	2010-01-05	6.8	CVE-2009-4572 XF BUGTRAQ MISC SECUNIA
qproje -- com_qpersonel	Cross-site scripting (XSS) vulnerability in the Q-Personel (com_qpersonel) component 1.0.2 RC2 for Joomla! allows remote attackers to inject arbitrary web script or HTML via the personel_sira parameter in a sirala action to index.php.	2010-01-06	4.3	CVE-2009-4575 XF BID OSVDB MISC SECUNIA
roseonlinecms -- roseonlinecms	Directory traversal vulnerability in modules/admincp.php in RoseOnlineCMS 3 B1 and earlier, when magic_quotes_gpc is disabled, allows remote attackers to include and execute arbitrary local files via directory traversal sequences in the admin parameter.	2010-01-06	6.8	CVE-2009-4581 XF BID MISC MISC
s2sys -- linear_emerge_access_control_system	Unspecified vulnerability in the management console in the S2 Security Linear eMerge Access Control System 2.5.x allows remote attackers to cause a denial of service (configuration reset) via a request to a crafted URI.	2010-01-05	5.0	CVE-2009-3734 CERT-VN MISC MISC
sandisk -- cruzer_enterprise_usb	SanDisk Cruzer Enterprise USB flash drives validate passwords with a program running on the host computer rather than the device hardware, which allows physically proximate attackers to access the cleartext drive contents via a modified program.	2010-01-07	4.6	CVE-2010-0224 MISC MISC MISC MISC MISC SECTRACK MISC MISC
sanDisk -- amzon_antemusic_usb	SanDisk Cruzer Enterprise USB flash drives do not prevent password replay attacks, which allows physically proximate attackers to access the	2010-01-06	4.6	CVE-2010-0226 MISC

sanDisk -- cruzer_enterprise_usb	cleartext drive contents by providing a key that was captured in a USB data stream at an earlier time.	07	4.0	MISC MISC MISC
scandisk -- cruzer_enterprise_usb	SanDisk Cruzer Enterprise USB flash drives use a fixed 256-bit key for obtaining access to the cleartext drive contents, which makes it easier for physically proximate attackers to read or modify data by determining and providing this key.	2010-01-07	4.6	CVE-2010-0225 MISC MISC MISC MISC MISC MISC MISC MISC
secureideas -- base	Cross-site scripting (XSS) vulnerability in base_local_rules.php in Basic Analysis and Security Engine (BASE) before 1.4.4 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2010-01-07	4.3	CVE-2009-4590 XF VUPEN CONFIRM SECUNIA CONFIRM
unleashedmind -- img_assist	The Image Assist module 5.x-1.x before 5.x-1.8, 5.x-2.x before 2.0-alpha4, 6.x-1.x before 6.x-1.1, 6.x-2.x before 2.0-alpha4, and 6.x-3.x-dev before 2009-07-15, a module for Drupal, does not properly enforce privilege requirements for unspecified pages, which allows remote attackers to read the (1) title or (2) body of an arbitrary node via unknown vectors.	2010-01-04	5.0	CVE-2009-4558 BID CONFIRM
verbatim -- corporate_secure	Verbatim Corporate Secure and Corporate Secure FIPS Edition USB flash drives validate passwords with a program running on the host computer rather than the device hardware, which allows physically proximate attackers to access the cleartext drive contents via a modified program.	2010-01-07	4.6	CVE-2010-0227 MISC MISC MISC SECTRACK MISC MISC
verbatim -- corporate_secure	Verbatim Corporate Secure and Corporate Secure FIPS Edition USB flash drives use a fixed 256-bit key for obtaining access to the cleartext drive contents, which makes it easier for physically proximate attackers to read or modify data by determining and providing this key.	2010-01-07	4.6	CVE-2010-0228 MISC MISC MISC MISC MISC
verbatim -- corporate_secure	Verbatim Corporate Secure and Corporate Secure FIPS Edition USB flash drives do not prevent password replay attacks, which allows physically proximate attackers to access the cleartext drive contents by providing a key that was captured in a USB data stream at an earlier time.	2010-01-07	4.6	CVE-2010-0229 MISC MISC
webmin -- usermin webmin -- webmin	Cross-site scripting (XSS) vulnerability in Webmin before 1.500 and Usermin before 1.430 allows remote attackers to inject arbitrary web script or HTML via unspecified vectors.	2010-01-05	4.3	CVE-2009-4568 CONFIRM VUPEN BID
worms-league -- webleague	Multiple SQL injection vulnerabilities in Admin/index.php in WebLeague 2.2.0, when magic_quotes_gpc is disabled, allow remote attackers to execute arbitrary SQL commands via	2010-01-04	6.8	CVE-2009-4561 XF MITIGATION

	the (1) username and (2) password parameters.		<a href="#">MILWORM</a>
wowd -- wowd	Multiple cross-site scripting (XSS) vulnerabilities in index.html in Wowd client before 1.3.1 allow remote attackers to inject arbitrary web script or HTML via the (1) sortby, (2) tags, or (3) ctx parameter in a search action.	2010-01-07	4.3 <a href="#">CVE-2009-4586</a> <a href="#">VUPEN</a> <a href="#">MISC</a> <a href="#">MISC</a>
zenphoto -- zenphoto	Cross-site scripting (XSS) vulnerability in zp-core/admin.php in Zenphoto 1.2.5 allows remote attackers to inject arbitrary web script or HTML via the from parameter.	2010-01-04	4.3 <a href="#">CVE-2009-4562</a> <a href="#">XF</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a> <a href="#">OSVDB</a>
zenphoto -- zenphoto	Cross-site request forgery (CSRF) vulnerability in zp-core/admin-options.php in Zenphoto 1.2.5 allows remote attackers to hijack the authentication of administrators for requests that change the administrative password via the o-adminpass and o-adminpass_2 parameters in a saveoptions action.	2010-01-04	4.3 <a href="#">CVE-2009-4563</a> <a href="#">XF</a> <a href="#">MILWORM</a> <a href="#">SECUNIA</a> <a href="#">OSVDB</a>
zenphoto -- zenphoto	SQL injection vulnerability in index.php in Zenphoto 1.2.5, when the ZenPage plugin is enabled, allows remote attackers to execute arbitrary SQL commands via the category parameter, related to a URI under news/category/.	2010-01-04	6.8 <a href="#">CVE-2009-4564</a> <a href="#">MILWORM</a>

[Back to top](#)

### Low Vulnerabilities

Primary Vendor -- Product	Description	Published	CVSS Score	Source & Patch Info
nanwich -- submitted_by	Cross-site scripting (XSS) vulnerability in the Submitted By module 6.x before 6.x-1.3 for Drupal allows remote authenticated users, with "administer content types" privileges, to inject arbitrary web script or HTML via an input string for "submitted by" text.	2010-01-04	3.5 <a href="#">CVE-2009-4559</a> <a href="#">CONFIRM</a>	
unleashedmind -- img_assist	Cross-site scripting (XSS) vulnerability in the Image Assist module 5.x-1.x before 5.x-1.8, 5.x-2.x before 2.0-alpha4, 6.x-1.x before 6.x-1.1, 6.x-2.x before 2.0-alpha4, and 6.x-3.x-dev before 2009-07-15, a module for Drupal, allows remote authenticated users, with image-node creation privileges, to inject arbitrary web script or HTML via a node title.	2010-01-04	2.1 <a href="#">CVE-2009-4557</a> <a href="#">BID</a> <a href="#">CONFIRM</a>	
viscacha -- viscacha	Multiple cross-site scripting (XSS) vulnerabilities in editprofile.php in Vischacha 0.8 Gold allow remote authenticated users to inject arbitrary web script or HTML via the (1) skype, (2) yahoo, (3) aol, (4) msn, or (5) jabber parameter in a profile2 action. NOTE: some of these details are obtained from third party information.	2010-01-05	3.5 <a href="#">CVE-2009-4567</a> <a href="#">XF</a> <a href="#">MISC</a> <a href="#">SECUNIA</a> <a href="#">MISC</a>	

[Back to top](#)

Last updated January 11, 2010

 Print This Document